Journal of Combinatorial Theory, Series A 116 (2009) 1120–1139

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Integral point sets in higher dimensional affine spaces over finite fields

Sascha Kurz, Harald Meyer

University of Bayreuth, Department of Mathematics, D-95440 Bayreuth, Germany

ARTICLE INFO

Article history:
Received 21 July 2008
Available online 25 March 2009

Keywords:
Finite geometry
Integral distances
Integral point sets
Automorphism group
Strongly regular graphs

ABSTRACT

We consider point sets in the m-dimensional affine space $\mathbb{F}_q^m$ where each squared Euclidean distance of two points is a square in $\mathbb{F}_q$. It turns out that the situation in $\mathbb{F}_q^m$ is rather similar to the one of integral distances in Euclidean spaces. Therefore we expect the results over finite fields to be useful for the Euclidean case.
We completely determine the automorphism group of these spaces which preserves integral distances. For some small parameters m and q we determine the maximum cardinality $\mathcal{I}(m,q)$ of integral point sets in $\mathbb{F}_q^m$. We provide upper bounds and lower bounds on $\mathcal{I}(m,q)$. If we map integral distances to edges in a graph, we can define a graph $\mathfrak{G}_{m,q}$ with vertex set $\mathbb{F}_q^m$. It turns out that $\mathfrak{G}_{m,q}$ is strongly regular for some cases.

1. Introduction and notation

Integral point sets, i.e. point sets with pairwise integral distances in Euclidean space, have been considered since the time of the Pythagoreans, who studied rectangles with integral side lengths and integral diagonal. Even nowadays there are a lot of unsolved problems concerning integral point sets [5, Section 5.11]. E.g. it is not known whether a perfect cuboid, that is a box with integer edges, face diagonals, and body diagonal, exists [8, Problem D18].

Applications originate from chemistry (molecules), physics (wave lengths), robotics, architecture, see [9]. The concept of integral point sets can be generalized to commutative rings in order to study the underlying structure suppressing number theoretical difficulties. Here, we consider point sets in m-dimensional affine space $\mathbb{F}_q^m$ where each squared Euclidean distance of two points is a square in $\mathbb{F}_q$.

E-mail addresses: sascha.kurz@uni-bayreuth.de (S. Kurz), harald.meyer@uni-bayreuth.de (H. Meyer).
URLs: http://www.wm.uni-bayreuth.de/index.php?id=sascha (S. Kurz),
http://www.old.uni-bayreuth.de/departments/math/org/mathe4/mit3.html (H. Meyer).

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2009.03.001

It turns out that the situation in $\mathbb{F}_q^m$ is rather similar to the one in Euclidean spaces. Therefore we expect the results over finite fields to be useful for the Euclidean case.

In this context we would like to remark the famous problem of P. Erdős who asked for seven points in the plane, no three on a line, no four on a circle with pairwise integral distances [8, Problem D20], [12]. Several conjectures and incorrect proofs circulated that such a point set cannot exist. In [14] the authors find corresponding examples over $\mathbb{F}_q^2$ consisting of nine points which finally lead to the discovery of an integral heptagon in the Euclidean plane in [15].

There has been done a lot of work on integral point sets in Euclidean spaces, see e.g. [9,15,16,18, 19]. Some authors also consider other spaces, e.g. Banach spaces [7], integral point sets over rings [14], or integral point sets over finite fields [1,6,11,17]. In [17] one of the authors of this article determines the automorphism group for dimension $m = 2$, and in [11] integral point sets over $\mathbb{F}_q^2$, which are maximal with respect to inclusion, were classified for $q \leqslant 47$. For $m = 2$ and $q \equiv 3 \pmod 4$ the graphs $\mathfrak{G}_{m,q}$ from Section 4 are isomorphic to Paley graphs of square order. So in some sense these graphs $\mathfrak{G}_{m,q}$ generalize Paley graphs. In [2] Blokhuis has determined the structure of cliques of maximal siz! e in Paley graphs of square order. Since, whenever two points in $\mathbb{F}_q^m$ are at integral distance the whole line through these points is an integral point set, integral point sets over $\mathbb{F}_q^m$ correspond to point sets with few directions being contained in a given set. From this point of view methods from Rédei's seminal work [21] can be applied to obtain results for point sets with few directions, see e.g. [3,4,22].

Here, after giving the basic facts on integral point sets over affine planes in Section 2, we completely determine the automorphism group of $\mathbb{F}_q^m$ with respect to integral distances in Theorem 3.2 and analyze its operation on $\mathbb{F}_q^m$ in Section 3. We introduce and analyze the graphs of integral distances $\mathfrak{G}_{m,q}$ for $m \geqslant 3$, $2 \nmid q$ in Section 4. They arise from 3-class association schemes. The determination of some of their parameters let us conjecture that they are strongly regular for even dimensions m. In Section 5 we consider the maximum cardinality $\mathcal{I}(m,q)$ of integral point sets over $\mathbb{F}_q^m$ and provide some new exact numbers for dimension $m = 3$. For general dimension m we state upper bounds and some constructions yielding lower bounds. We finish with a conclusion and an outlook in Section 6.

We end this introduction with some notation we will keep throughout the paper. Let p be a prime and let $q = p^r$ be a power. We write $\mathbb{F}_q$ for the field with q elements and $\mathbb{F}_q^* := \mathbb{F}_q \backslash \{0\}$ for the units of $\mathbb{F}_q$. Our notation for the general linear group, i.e. the set of invertible m by m matrices over $\mathbb{F}_q$, is $GL(m,q)$. By

$$O(m,q) := \left\{ A \in GL(m,q) \;\middle|\; A^T A = A A^T = E^{(m)} \right\},$$

where $E^{(m)}$ is the $m \times m$ identity matrix, we denote the orthogonal group in dimension m. We remark that for even dimension $2n$ the orthogonal group comes in two types $O^+(2n,q)$ and $O^-(2n,q)$, and the group we defined above is isomorphic to $O^+(2n,q)$ in this case. By $A\Gamma L(m,q)$ we denote the affine general semilinear group over $\mathbb{F}_q$ and by

$$OZ(m,q) := \left\{ A \in GL(m,q) \;\middle|\; A^T A = A A^T \in \mathbb{F}_q^* \cdot E^{(m)} \right\},$$

we denote the smallest group containing $O(m,q)$ and the center of $GL(m,q)$, i.e. the diagonal matrices with equal entries at the diagonal.

Originally integral point sets were defined in m-dimensional Euclidean spaces $\mathbb{E}^m$ as sets of n points with pairwise integral distances in the Euclidean metric, see e.g. [9,15,16,18,19] for an overview on the most recent results. Here we consider integral point sets in the affine spaces $\mathbb{F}_q^m$. We equip those spaces with a bilinear form

$$\langle u, v \rangle := u^T v = \sum_{i=1}^{m} u_i v_i$$

and a squared distance

$$d^2(u,v) := \langle u - v, u - v \rangle = (u-v)^T (u-v) = \sum_{i=1}^{m} (u_i - v_i)^2 \quad \in \mathbb{F}_q$$

for any two points $u=(u_1\ \cdots\ u_m)^T$, $v=(v_1\ \cdots\ v_m)^T$ in $\mathbb{F}_q^m$. We say that two points $u,v\in\mathbb{F}_q^m$ are at integral distance if $d^2(u,v)$ is contained in the set $\square_q:=\{\alpha^2\mid\alpha\in\mathbb{F}_q\}$ consisting of the squares in $\mathbb{F}_q$. As in the Euclidean space we define the cross product of two vectors $u,v\in\mathbb{F}_q^3$ by

$$u\times v:=\big((u_2v_3-u_3v_2)\quad(-u_1v_3+u_3v_1)\quad(u_1v_2-u_2v_1)\big)^T\in\mathbb{F}_q^3.$$

The proofs of some of the common formulas for the cross product do not depend on any specific attributes of the Euclidean space, so they still hold in $\mathbb{F}_q^3$. Especially this is true for the formulas

$$\langle u\times v,u\rangle=\langle u\times v,v\rangle=0$$

and

$$\langle u\times v,u\times v\rangle=\langle u,u\rangle\cdot\langle v,v\rangle-\langle u,v\rangle^2$$

we will use later on. The notation

$$U^\perp:=\big\{v\in\mathbb{F}_q^m\ \big|\ \langle u,v\rangle=0\text{ for all }u\in U\big\}$$

for a subspace $U\subseteq\mathbb{F}_q^m$ is also inspired by the notation for the Euclidean space. As a shorthand we use $u^\perp$ instead of $\{u\}^\perp$ for a vector $u\in\mathbb{F}_q^m$.

We have the equation

$$\langle Au,Av\rangle=(Au)^T(Av)=u^TA^TAv=u^Tv=\langle u,v\rangle$$

for all $u,v\in\mathbb{F}_q^m$ and all $A\in O(m,q)$. If we have a matrix $A\in GL(m,q)$ with $\langle Au,Av\rangle=\langle u,v\rangle$ for all $u,v\in\mathbb{F}_q^m$, then we have

$$u^TA^TAv=(Au)^T(Av)=\langle Au,Av\rangle=\langle u,v\rangle=u^Tv$$

for all $u,v\in\mathbb{F}_q^m$, i.e. $A^TA=E^{(m)}$ and so A is an element of $O(m,q)$.

2. Integral point sets

A set $\mathbb{P}$ of points in $\mathbb{F}_q^m$ is called an integral point set if all pairs of points are at integral distance, i.e. if $d^2(u,v)\in\square_q$ for all $u,v\in\mathbb{P}$. As a shorthand we define $\Delta:\mathbb{F}_q^m\times\mathbb{F}_q^m\to\{0,1\}$,

$$(u,v)\mapsto\begin{cases}1 & \text{if } u \text{ and } v \text{ are at integral distance,}\\ 0 & \text{otherwise.}\end{cases}$$

By $\mathcal{I}(m,q)$ we denote the maximum cardinality of an integral point set in $\mathbb{F}_q^m$.

Lemma 2.1.

$$q\leqslant\mathcal{I}(m,q)\leqslant q^m.$$

Proof. For the lower bound we consider the *line* $\mathbb{P}=\{(\alpha\ 0\ \cdots\ 0)^T\mid\alpha\in\mathbb{F}_q\}$. □

Lemma 2.2. *If $2\mid q$ then we have $\mathcal{I}(m,q)=q^m$.*

Proof. For two points $u=(u_1\ \cdots\ u_m)^T$, $v=(v_1\ \cdots\ v_m)^T$ in $\mathbb{F}_q^m$ we have

$$d^2(u,v)=\sum_{i=1}^m(u_i-v_i)^2=\underbrace{\left(\sum_{i=1}^m u_i+v_i\right)^2}_{\in\mathbb{F}_q}.\qquad\square$$

So in the remaining part of this article we consider only the cases where $2 \nmid q$.
The lower bound of Lemma 2.1 is attained in some cases, too, see e.g. [17] for a proof:

Theorem 2.3.

$$\mathcal{I}(2,q) = q \quad \text{for } 2 \nmid q.$$

3. Automorphisms preserving integral distances

The primary object of this section is to determine the automorphism group of $\mathbb{F}_q^m$ with respect to Δ. We first have to define what we consider as an automorphism.

Definition 3.1. *An automorphism of $\mathbb{F}_q^m$ with respect to Δ is a bijective mapping $\varphi \in A\Gamma L(\mathbb{F}_q, m)$ with*

$$\Delta(u,v) = \Delta\big(\varphi(u), \varphi(v)\big)$$

for all $u, v \in \mathbb{F}_q^m$. The group of automorphisms with respect to Δ is denoted by $\mathrm{Aut}(m,q)$.

In other words this definition says that φ has to map affine subspaces, like points, lines, or hyperplanes, to affine subspaces with equal dimension, and has to preserve the integral distance property. It is easy to find the automorphisms with respect to Δ, see Lemma 3.8. The difficult part is to show that these are all automorphisms for $m \geqslant 3$. Here, the translations and Frobenius homomorphisms do not cause any problems, so the most important part of the determination of the automorphism group is to determine the linear automorphisms. The main theorem of this section is:

Theorem 3.2.

$$\mathrm{Aut}(m,q) \cap GL(m,q) = OZ(m,q) \quad \text{for } 2 \nmid q \text{ and } m \geqslant 3.$$

The idea of the proof of this theorem is to do induction using the results for the case of dimension $m = 2$ one of the authors achieved in [17]. But for the proof we need a lot of facts about squares in and about the action of the automorphism group on $\mathbb{F}_q^m$. We will prove these facts step by step in several lemmas. We start with some statements about roots in $\mathbb{F}_q$ and the set of solutions of quadratic equations in $\mathbb{F}_q$.

Definition 3.3. *Let $q \equiv 1 \bmod 4$. By ω_q we denote an element with $\omega_q^2 = -1$.*

Lemma 3.4. *For a finite field $\mathbb{F}_q$ with $q = p^r$ and $p \neq 2$ we have $-1 \in \square_q$ iff $q \equiv 1 \bmod 4$, $\omega_q \in \square_q$ iff $q \equiv 1 \bmod 8$, and $2 \in \square_q$ iff $q \equiv \pm 1 \bmod 8$.*

Proof. The multiplicative group of the units $\mathbb{F}_q^*$ is cyclic of order $q-1$. Elements of order 4 are exactly those elements α with $\alpha^2 = -1$. A similar argument holds for the fourth roots of -1. For the last statement we have to generalize the second auxiliary theorem (Ergänzungssatz) of the quadratic reciprocity law to $\mathbb{F}_q$: If $q = p$ is prime then the statement is true by the second auxiliary theorem. If 2 is a square in $\mathbb{F}_p$ then 2 is also a square in $\mathbb{F}_{p^r}$ and from $p \equiv \pm 1 \bmod 8$ we get $q = p^r \equiv \pm 1 \bmod 8$, i.e. the statement is true in this case. If 2 is not a square in $\mathbb{F}_p$ then the polynomial $x^2 - 2 \in \mathbb{F}_p[x]$ is irreducible and 2 is a square in $\mathbb{F}_p[x]/(x^2-2) \cong \mathbb{F}_{p^2}$. Hence 2 is a square in $\mathbb{F}_{p^k}$ iff $2 \mid k$. As p is an odd prime with $p \equiv \pm 3 \bmod 8$ we obtain $p^2 \equiv 1 \bmod 8$ and also $p^{2k} \equiv 1 \bmod 8$ as well as $p^{2k+1} \equiv \pm 3$ in this case. □

Definition 3.5. *A triple (α, β, γ) is called* Pythagorean triple over $\mathbb{F}_q$ *if $\alpha^2 + \beta^2 = \gamma^2$.*

In the following it will be useful to have a parametric representation of the Pythagorean triples over $\mathbb{F}_q$.

Lemma 3.6. *For $2 \nmid q$ let $\gamma \in \mathbb{F}_q$ and let $\mathbb{H}_\gamma$ be the set of Pythagorean triples (α, β, γ) over $\mathbb{F}_q$.*

(a) *If $\gamma = 0$ then*

$$\mathbb{H}_0 = \begin{cases} \{(\tau, \pm\tau\omega_q, 0) \mid \tau \in \mathbb{F}_q\} & \text{if } q \equiv 1 \pmod 4, \\ \{(0,0,0)\} & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

and

$$|\mathbb{H}_0| = \begin{cases} 2q-1 & \text{if } q \equiv 1 \pmod 4, \\ 1 & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

(b) *If $\gamma \neq 0$ then*

$$\mathbb{H}_\gamma = \{(\pm\gamma, 0, \gamma)\} \cup \{(0, \pm\gamma, \gamma)\} \cup \left\{ \left(\frac{\tau^2-1}{\tau^2+1} \cdot \gamma, \frac{2\tau}{\tau^2+1} \cdot \gamma, \gamma \right) \;\middle|\; \tau \in \mathbb{F}_q^*,\ \tau^2 \neq \pm 1 \right\}$$

and

$$|\mathbb{H}_\gamma| = \begin{cases} q-1 & \text{if } q \equiv 1 \pmod 4, \\ q+1 & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

(c) *There are exactly q^2 Pythagorean triples over $\mathbb{F}_q$.*

Proof. Part (a) is easy to verify. For part (b) there are 4 solutions with $\alpha\beta = 0$, these are $\{(0, \pm\gamma, \gamma), (\pm\gamma, 0, \gamma)\}$. For $\alpha\beta \neq 0$ we get:

$$\alpha^2 + \beta^2 = \gamma^2 \quad \Leftrightarrow \quad \frac{\gamma - \alpha}{\beta} \cdot \frac{\gamma + \alpha}{\beta} = 1.$$

Setting $\tau := \frac{\gamma+\alpha}{\beta} \in \mathbb{F}_q^*$ we obtain $\tau^{-1} = \frac{\gamma-\alpha}{\beta}$, hence

$$\frac{\alpha}{\beta} = \frac{\tau - \tau^{-1}}{2} \quad \text{and} \quad \frac{\gamma}{\beta} = \frac{\tau + \tau^{-1}}{2}.$$

Because of $\alpha \neq 0$, $\gamma \neq 0$ we have $\tau \neq \pm\tau^{-1}$, i.e. $\tau^2 \notin \{-1, 1\}$. It follows

$$\alpha = \frac{\tau - \tau^{-1}}{\tau + \tau^{-1}} \cdot \gamma \quad \text{and} \quad \beta = \frac{2}{\tau + \tau^{-1}} \cdot \gamma.$$

It is easily checked that for all admissible values of τ, the resulting triples (α, β, γ) are pairwise different Pythagorean triples.

The expression for the number of solutions follows because -1 is a square in $\mathbb{F}_q$ exactly if $q \equiv 1 \pmod 4$.

With parts (a) and (b) we get the number of Pythagorean triples over $\mathbb{F}_q$ as

$$\sum_{\gamma \in \mathbb{F}_q} |\mathbb{H}_\gamma| = |\mathbb{H}_0| + (q-1) \cdot |\mathbb{H}_1| = q^2.$$

So also part (c) is shown. □

From this lemma we can deduce the following corollary.

Corollary 3.7. *If $\mathbb{I}_\gamma := \{(\alpha, \beta) \mid \alpha^2 + \beta^2 = \gamma\}$ then we have*

$$|\mathbb{I}_0| = \begin{cases} 2q-1 & \text{if } q \equiv 1 \pmod 4, \\ 1 & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

and

$$|\mathbb{I}_\gamma| = \begin{cases} q-1 & \text{if } q \equiv 1 \pmod 4, \\ q+1 & \text{if } q \equiv 3 \pmod 4 \end{cases}$$

for $\gamma \neq 0$.

Proof. For $\gamma \in \square_q$ (this includes $\gamma = 0$) the formulas were proven in Lemma 3.6. So let $\gamma \in \mathbb{F}_q$ be a non-square. As the squares $\square_q \backslash \{0\}$ form a subgroup of $\mathbb{F}_q^*$, the non-squares have the form $\gamma \cdot \delta^2$ with $\delta \neq 0$. If $\alpha^2 + \beta^2 = \gamma$ then $(\alpha\delta)^2 + (\beta\delta)^2 = \gamma\delta^2$. Therefore the number of solutions (α, β) is the same for all non-squares and we can determine the number of solutions by counting: There are q^2 pairs $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$. As there are $\frac{q-1}{2}$ squares and non-squares in $\mathbb{F}_q^*$ we obtain

$$\frac{q-1}{2} \cdot |\mathbb{I}_\gamma| = q^2 - (2q-1) - \frac{q-1}{2} \cdot (q-1) = \frac{1}{2}q^2 - q + \frac{1}{2} = \frac{1}{2}(q-1)^2$$

for $q \equiv 1 \pmod 4$ and

$$\frac{q-1}{2} \cdot |\mathbb{I}_\gamma| = q^2 - 1 - \frac{q-1}{2} \cdot (q+1) = \frac{1}{2}(q-1)(q+1)$$

for $q \equiv 3 \pmod 4$, which yields our statement. □

Now we want to study the automorphism group of $\mathbb{F}_q^m$ with respect to Δ. As already mentioned it is easy to determine the automorphisms:

Lemma 3.8. *Examples of automorphisms of* $\mathbb{F}_q^m$ *with respect to* Δ *are given by*:

(1) $\varphi_v(u) = (u_1 + v_1 \ \cdots \ u_m + v_m)^T$ *for* $v \in \mathbb{F}_q^m$,
(2) $\tilde{\varphi}_\alpha(u) = \alpha \cdot u$ *for* $\alpha \in \mathbb{F}_q^*$,
(3) $\tilde{\varphi}_A(u) = A \cdot u$ *for* $A \in O(m, q)$, *and*
(4) $\hat{\varphi}_i(u) = \left(u_1^{p^i} \ \cdots \ u_m^{p^i}\right)^T$ *for* $i \in \{1, \ldots, r-1\}$ *and* $q = p^r$.

Proof. The first two cases are easy to check. For the third case we consider

$$\begin{aligned} d^2(Au, Av) &= \langle A(u-v), A(u-v) \rangle = (u-v)^T A^T A(u-v) \\ &= (u-v)^T (u-v) = \langle u-v, u-v \rangle = d^2(u, v) \end{aligned}$$

and for the fourth case we have

$$d^2\left(\hat{\varphi}_i(0), \hat{\varphi}_i(u)\right) = \sum_{j=1}^m \left(u_j^{p^i}\right)^2 = \sum_{j=1}^m \left(u_j^2\right)^{p^i} = \left(\sum_{j=1}^m u_j^2\right)^{p^i} = d^2(0, u)^{p^i}. \qquad \square$$

We would like to remark that the orders of the groups $O(m, q)$, $GL(m, q)$, and $OZ(m, q)$ are as follows:

(1) $|GL(m, q)| = \prod_{i=0}^{m-1} (q^m - q^i)$ for all $m \in \mathbb{N}$.
(2) $|O(2n+1, q)| = 2q^n \cdot \prod_{i=0}^{n-1} (q^{2n} - q^{2i})$ for $n \in \mathbb{N}$.
(3) $|O(2n, q)| = 2(q^n - 1) \cdot \prod_{i=1}^{n-1} (q^{2n} - q^{2i})$ for $n \in \mathbb{N}$ and $-1 \in \square_q$.
(4) $|O(2n, q)| = 2(q^n + (-1)^{n+1}) \cdot \prod_{i=1}^{n-1} (q^{2n} - q^{2i})$ for $n \in \mathbb{N}$ and $-1 \notin \square_q$.
(5) $|OZ(m, q)| = \frac{q-1}{2} \cdot |O(m, q)|$ for all $m \in \mathbb{N} \backslash \{1\}$.

As the Frobenius homomorphisms and the translations are automorphisms with respect to Δ it suffices to determine the matrix group $\mathrm{Aut}(m,q) \cap GL(m,q)$ of all matrices that are automorphisms with respect to Δ in order to determine the whole automorphism group. Due to Lemma 3.8 we have $OZ(m,q) \leqslant \mathrm{Aut}(m,q) \cap GL(m,q)$. Thus for dimension $m = 3$ we have $(q-1)^2 q(q+1) \mid |\mathrm{Aut}(3,q) \cap GL(3,q)|$. We will prove later on that $OZ(3,q)$ is already isomorphic to $\mathrm{Aut}(3,q) \cap GL(3,q)$.

Firstly we summarize our knowledge on $\mathrm{Aut}(m,q)$:

Theorem 3.9. *We have*

(1) $\mathrm{Aut}(m,q) = A\Gamma L(m,q)$ *for* $2 \mid q$,
(2) $\mathrm{Aut}(1,q) = A\Gamma L(1,q)$,
(3) $\mathrm{Aut}(2,q) \cap GL(2,q) = OZ(2,q)$ *for* $2 \nmid q$, $q \notin \{5,9\}$,
(4) $\mathrm{Aut}(2,5) \cap GL(2,5) > OZ(2,5)$, $\frac{|\mathrm{Aut}(2,5) \cap GL(2,5)|}{|OZ(2,5)|} = 2$, *and*
(5) $\mathrm{Aut}(2,9) \cap GL(2,9) > OZ(2,9)$, $\frac{|\mathrm{Aut}(2,9) \cap GL(2,9)|}{|OZ(2,9)|} = 3$.

Proof. (1) and (2) hold as for $m = 1$ or $2 \mid q$ all distances are integral. So in general we assume dimension $m \geqslant 2$ and odd characteristic $2 \nmid q$ if not stated otherwise in the rest of this article. For the proof of (3)–(5) we refer to [17]. □

Next we prove some results on the orbits of $\mathbb{F}_q^m$ under the groups $O(m,q)$ and $OZ(m,q)$. Therefore we need:

Definition 3.10. *By $\mathbb{P}_\tau$ we denote the set $\{u \in \mathbb{F}_q^m \setminus \{0\} \mid d^2(0,u) = \tau\}$, where the parameters q and m are provided by the context.*

Lemma 3.11. *For every $\tau \in \mathbb{F}_q$ the group $O(2,q)$ acts transitively on $\mathbb{P}_\tau$.*

Proof. Firstly we consider $\tau \neq 0$. Therefore let $u = (u_1\ u_2)^T$ and $v = (v_1\ v_2)^T$ be two points in $\mathbb{F}_q^2$ with $u_1^2 + u_2^2 = v_1^2 + v_2^2 = \tau \neq 0$. With $\alpha = \frac{u_1 v_1 + u_2 v_2}{\tau}$ and $\beta = \frac{u_2 v_1 - u_1 v_2}{\tau}$ we have $\alpha^2 + \beta^2 = \frac{(u_1^2+u_2^2)\cdot(v_1^2+v_2^2)}{\tau^2} = 1$. Thus the matrix $A = \left(\begin{smallmatrix} \alpha & \beta \\ -\beta & \alpha \end{smallmatrix}\right)$ is an element of $O(2,q)$ which maps u to v.

Now we deal with the remaining case $\tau = 0$. If $-1 \notin \square_q$ then we have $|\mathbb{P}_0| = 0$. Thus we may assume $-1 \in \square_q$. For $\alpha, \beta \in \mathbb{F}_q$ with $\alpha^2 + \beta^2 = 0$ we have either $\alpha = \beta = 0$ or $\alpha, \beta \neq 0$. In the latter case we have $(\frac{\alpha}{\beta})^2 = -1$, which has two solutions $\frac{\alpha}{\beta} = \omega_q$ and $\frac{\alpha}{\beta} = -\omega_q$, where ω_q is a square root of -1. Thus we can write all elements of $\mathbb{P}_0$ as $(\nu\ \pm\nu\omega_q)^T$ with $\nu \in \mathbb{F}_q^*$. Now we apply all matrices of the form $B := \left(\begin{smallmatrix} \gamma & \delta \\ -\delta & \gamma \end{smallmatrix}\right)$ with $\gamma^2 + \delta^2 = 1$ to the vector $(1\ \omega_q)^T$. By definition these matrices are elements of $O(2,q)$. If we parameterize γ and δ as in Lemma 3.6 we get $B(1\ \omega_q)^T = (\nu\ \nu\omega_q)^T$, where $\nu = \frac{\tau - \tau^{-1}}{\tau + \tau^{-1}} + \frac{2}{\tau + \tau^{-1}} \cdot \omega_q$. By a small computation we check that

$$f : \mathbb{F}_q \setminus \{0, \omega_q, -\omega_q\} \to \mathbb{F}_q \setminus \{-1, 0, 1\}, \qquad \tau \mapsto \frac{\tau - \tau^{-1}}{\tau + \tau^{-1}} + \frac{2}{\tau + \tau^{-1}} \cdot \omega_q$$

are well defined and injective. Thus all points $(\nu\ \nu\omega_q)^T$ are in the same orbit as $(1\ \omega_q)^T$ under the action of $O(2,q)$. As $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in O(2,q)$, the points $(\nu\ -\nu\omega_q)^T$ are also contained in this orbit and the proposed statement holds. □

Lemma 3.12. *For each $u \in \mathbb{F}_q^3$ with $u_1^2 + u_2^2 + u_3^2 = 1$ there exist $v = (v_1\ v_2\ v_3)^T$, $w = (w_1\ w_2\ w_3)^T \in \mathbb{F}_q^3$ fulfilling $v_1^2 + v_2^2 + v_3^2 = w_1^2 + w_2^2 + w_3^2 = 1$, such that $\langle u, v\rangle = \langle u, w\rangle = \langle v, w\rangle = 0$.*

Proof. The set $u^\perp$ of vectors $\tilde{v}$ solving the linear equation $\langle \tilde{v}, u\rangle = 0$ forms a 2-dimensional vector space. Let $\tilde{v} \in u^\perp$ be an arbitrary element with $\tilde{v} \neq 0$. Then $\tilde{v}^\perp$ is also a 2-dimensional vector

space and certainly $u \in \tilde{v}^{\perp}$. Thus we get $\tilde{v}^{\perp} \neq u^{\perp}$. Therefore the orthogonal vector space $u^{\perp}$ is non-degenerate in the sense of [10, II.10.1]. By [10, II.10.2(b)] there is an orthogonal basis $\{\hat{v}, \hat{w}\}$ of $u^{\perp}$, i.e. we have $\langle \hat{v}, \hat{w}\rangle = 0$ and $\langle \hat{v}, \hat{v}\rangle$, $\langle \hat{w}, \hat{w}\rangle \neq 0$. For $\alpha, \beta \in \mathbb{F}_q$ we obtain

$$\langle \alpha\hat{v} + \beta\hat{w}, \alpha\hat{v} + \beta\hat{w}\rangle = \alpha^2\langle \hat{v}, \hat{v}\rangle + \beta^2\langle \hat{w}, \hat{w}\rangle.$$

As $\langle \hat{v}, \hat{v}\rangle, \langle \hat{w}, \hat{w}\rangle \in \mathbb{F}_q^*$ there exists $\alpha, \beta \in \mathbb{F}_q$ such that

$$\langle \alpha\hat{v} + \beta\hat{w}, \alpha\hat{v} + \beta\hat{w}\rangle = 1$$

by [23, Lemma 11.1]. Therefore there is a vector $v \in \mathbb{F}_q^3$ such that $\langle u, v\rangle = 0$ and $\langle v, v\rangle = 1$. Now w can easily be constructed: The cross product $w := u \times v$ is a vector with $\langle u, w\rangle = \langle v, w\rangle = 0$ and

$$\langle w, w\rangle = \langle u, u\rangle \cdot \langle v, v\rangle - \langle u, v\rangle^2 = 1. \qquad \square$$

From the previous lemma we can easily deduce:

Lemma 3.13. *The group $O(3, q)$ acts transitively on $\mathbb{P}_\tau$ for all $\tau \in \mathbb{F}_q$.*

Proof. For $\tau = 0$ we refer to [23, Theorem 11.6]. Thus we may assume $\tau \neq 0$. Firstly we consider $\tau \in \square_q$. Let $\tilde{u} \in \mathbb{F}_q^3$ such that $\langle \tilde{u}, \tilde{u}\rangle = \nu^2 = \tau \neq 0$. We put $u := \nu^{-1}\tilde{u}$. Then $\langle u, u\rangle = 1$ and by Lemma 3.12 there are $v, w \in \mathbb{F}_q^3$ such that $A = (u\ v\ w)$ is an orthogonal matrix. Thus the vectors $(1\ 0\ 0)^T$ and u are in the same orbit of $O(3, q)$. Thus all $\tilde{u}$ with $\langle \tilde{u}, \tilde{u}\rangle = \nu^2 \neq 0$ and the vectors $(\pm\nu\ 0\ 0)$ are in the same orbit.

Now we deal with the remaining cases $\tau \notin \square_q$. Let $u \in \mathbb{P}_\tau$ be an arbitrary vector. We show that there exists an element $A \in O(3, q)$ such that the third coordinate of Au is equal to zero. This reduces the problem to the 2-dimensional case where we can apply Lemma 3.11, as we can extend a 2-dimensional matrix $A' \in O(2, q)$ to a matrix $A \in O(3, q)$ by adding a third row and a third column consisting of a one in the diagonal and zeros elsewhere.

If $u_2^2 + u_3^2 = \nu^2 \neq 0$ then due to Lemma 3.11 there is an element $A' \in O(2, q)$ which maps $(u_2\ u_3)^T$ to $(\nu\ 0)^T$. Thus we can extend A' to a desired matrix $A \in O(3, q)$ such that the third coordinate of Au is equal to zero. Since $u_1^2 + u_2^2 + u_3^2 \notin \square_q$ we cannot have $u_i^2 + u_j^2 = 0$ for $i \neq j$. So we can assume $u_i^2 + u_j^2 \notin \square_q$ for $i \neq j$.

For the remaining cases we use another technique. We set

$$\mathbb{P}_{\tau,\mu} := \left\{ v \in \mathbb{F}_q^3 \backslash \{0\} \;\middle|\; v_1 = \mu,\ v_1^2 + v_2^2 + v_3^2 = \tau \right\}.$$

By Lemma 3.11 all points of $\mathbb{P}_{\tau,\mu}$ are contained in the same orbit under $O(3, q)$. From Corollary 3.7 we deduce $|\mathbb{P}_{\tau,\mu}| = q - 1$ for $q \equiv 1 \pmod 4$ and $|\mathbb{P}_{\tau,\mu}| = q + 1$ for $q \equiv 3 \pmod 4$. Hence we have

$$|\mathbb{P}_\tau| = \sum_{\mu \in \mathbb{F}_q} |\mathbb{P}_{\tau,\mu}| = q \cdot |\mathbb{P}_{\tau,0}|.$$

Now let us consider an arbitrary point $v \in \mathbb{P}_{\tau,\mu}$ and set $\lambda = v_1^2 + v_2^2$. As $v_1^2 + v_2^2 + v_3^2 = \tau \notin \square_q$ we have $\lambda \neq 0$. Due to Lemma 3.11 all points $w \in \mathbb{F}_q^3$ with $w_1^2 + w_2^2 = \lambda$ lie in the same orbit as v under $O(3, q)$.

Due to Corollary 3.7 we have at least $q + 1$ solutions (u_1, u_2) of the equation $u_1^2 + u_2^2 = \lambda$ for $q \equiv 3 \pmod 4$ and $\frac{q+1}{2}$ of the u_1 are pairwise different. This means that every point in $\mathbb{P}_\tau$ lies in an orbit with at least $\frac{q+1}{2} \cdot |\mathbb{P}_{\tau,u_1}| = \frac{(q+1)^2}{2} > \frac{|\mathbb{P}_\tau|}{2} = \frac{q(q+1)}{2}$ points. Thus there can only be one orbit.

For $q \equiv 1 \pmod 4$ we similarly conclude that every point in $\mathbb{P}_\tau$ lies in an orbit with at least $\frac{(q-1)^2}{2}$ points. As $|\mathbb{P}_\tau| = (q-1)q$ and $|\mathbb{P}_{\tau,\mu}| = q - 1$ for all $\mu \in \mathbb{F}_q$ there can exist two orbits at most and the length of every orbit has to be divisible by $|\mathbb{P}_{\tau,\mu}| = q - 1$. If there exist exactly two orbits $\mathbb{B}_1$, $\mathbb{B}_2$ then we have w.l.o.g. $|\mathbb{B}_1| = \frac{q-1}{2} \cdot (q-1)$ and $|\mathbb{B}_2| = \frac{q+1}{2} \cdot (q-1)$. Due to $|\mathbb{B}_1|\,|\,|O(3, q)|$ we have

$(q-1)^2 \mid 4\cdot(q-1)q(q+1)$. Using $\gcd(q-1,q)=1$ we conclude $q-1 \mid 4(q+1)$. Thus we have $q-1 \mid 8$, which is equivalent to $q \in \{3,5,9\}$. As $3 \not\equiv 1 \pmod 4$ we only have to consider the cases $q=9$ and $q=5$. In $\mathbb{F}_9 \simeq \mathbb{F}_3[x]/(x^2+1)$ we have $\square_9 = \{0,1,2,x,2x\}$. As we have either $v_i = 0$ for some i or $|\{v_1,v_2,v_3\} \cap \{1,2\}| \geqslant 2$ or $|\{v_1,v_2,v_3\} \cap \{x,2x\}| \geqslant 2$ there exist i,j with $v_i^2 + v_j^2 \in \square_9$ in this case and we can apply our reduction to the 2-dimensional case.

For $q=5$, $\tau=2$ we have

$$\mathbb{B}_1 = \left\{ (v_1 \quad v_2 \quad v_3)^T \mid v_1,v_2,v_3 \in \{2,3\} \right\},$$
$$\mathbb{B}_2 = \left\{ (0 \quad v_1 \quad v_2)^T, (v_1 \quad 0 \quad v_2)^T, (v_1 \quad v_2 \quad 0)^T \mid v_1,v_2 \in \{1,4\} \right\},$$

and for $q=5$, $\tau=3$ we have

$$\mathbb{B}_1 = \left\{ (v_1 \quad v_2 \quad v_3)^T \mid v_1,v_2,v_3 \in \{1,4\} \right\},$$
$$\mathbb{B}_2 = \left\{ (0 \quad v_1 \quad v_2)^T, (v_1 \quad 0 \quad v_2)^T, (v_1 \quad v_2 \quad 0)^T \mid v_1,v_2 \in \{2,3\} \right\}.$$

By considering the matrix $B = \begin{pmatrix} 1&2&4 \\ 2&1&4 \\ 1&1&3 \end{pmatrix}$ in $O(3,5)$ we conclude that in both cases $\mathbb{B}_1$ and $\mathbb{B}_2$ are contained in the same orbit. □

Lemma 3.14. *For dimension $m \geqslant 4$ and $u \in \mathbb{F}_q^m$ there exists an element $A \in O(m,q)$ such that the mth coordinate of Au is equal to zero.*

Proof. If one of the u_i is equal to zero then there obviously exists such a matrix A. So we assume $u_i \neq 0$ for $1 \leqslant i \leqslant m$.

If $u_h^2 + u_i^2 + u_j^2 = 0$ for all pairwise different $1 \leqslant h,i,j \leqslant m$ then we would have $u=0$ or $3 \mid q$: As $m \geqslant 4$, there is at least one further index k. If we replace u_h by u_k then $u_k^2 + u_i^2 + u_j^2 = 0$ and $u_h^2 + u_i^2 + u_j^2 = 0$ results in $u_h^2 = u_k^2$. Replacing u_i and u_j by u_k leads to $u_h^2 = u_i^2 = u_j^2 = u_k^2$, so we obtain $3u_i^2 = 0$ and thus $u=0$ if $3 \nmid q$.

For $3 \mid q$ the same computation leads to $u_i = \pm u_j$ for all i,j. W.l.o.g. let $u_1 = 1$. Then we have $u_i^2 + u_j^2 = 2$ for all $i,j > 1$. By Lemma 3.11 the group $O(2,q)$ acts transitively on $\mathbb{P}_2$. As we can extend 2-dimensional orthogonal matrices by ones in the diagonal we can assume $u_i = 1$ for $1 \leqslant i \leqslant m$. As the matrix

$$A' = \begin{pmatrix} 1&1&1&1 \\ 1&1&2&2 \\ 1&2&1&2 \\ 1&2&2&1 \end{pmatrix} \in O(4,q)$$

maps $(1\ 1\ 1\ 1)^T$ to $(1\ 0\ 0\ 0)^T$, we can extend A' to a matrix A in $O(m,q)$ such that Au has a zero at coordinate m.

So we may assume $0 \neq u_{m-2}^2 + u_{m-1}^2 + u_m^2 =: \mu$. As there exist $\alpha,\beta \in \mathbb{F}_q$ with $\alpha^2 + \beta^2 = \mu \neq 0$ by [23, Lemma 11.1] we can apply Lemma 3.13 to deduce that there exists an element $A' \in O(3,q)$ which maps $(u_{m-2}\ u_{m-1}\ u_m)^T$ onto $(\alpha\ \beta\ 0)^T$. Clearly we can extend A' to obtain the desired matrix $A \in O(m,q)$ mapping v onto a point with mth coordinate being equal to zero. □

Theorem 3.15. *For dimension $m \geqslant 2$ the group $O(m,q)$ acts transitively on $\mathbb{P}_\tau$ for all $\tau \in \mathbb{F}_q$.*

Proof. We prove the theorem by induction and use Lemmas 3.11 and 3.13 as induction basis. Now let $u,v \in \mathbb{P}_\tau$ be arbitrary. Due to Lemma 3.14 there exists $A,B \in O(m,k)$ such that the mth coordinate of $\tilde{u} = Au$ and the mth coordinate of $\tilde{v} = Bv$ are both equal to zero. Deleting the last coordinate from $\tilde{u}$ and $\tilde{v}$ yields two vectors $\hat{u}$ and $\hat{v}$ in $\mathbb{P}_\tau$, respectively. Due to our induction hypothesis there exists an element $C' \in O(m-1,q)$ with $C'\hat{u} = \hat{v}$. Clearly we can extend C' to a matrix $C \in O(m,q)$ with $C\tilde{u} = \tilde{v}$. With $D = B^{-1}CA$ we have $D \in O(m,q)$ and $Du = v$. □

Definition 3.16. *We set*

$$\mathbb{P}^+ := \bigcup_{\tau\in\square_q\setminus\{0\}} \mathbb{P}_\tau \quad \text{and} \quad \mathbb{P}^- := \bigcup_{\tau\notin\square_q} \mathbb{P}_\tau.$$

Lemma 3.17. *For $2\nmid q$ and $m\geqslant 2$ the orbits of $\mathbb{F}_q^m$ under the group $OZ(m,q)$ are $\mathbb{P}^+$, $\mathbb{P}_0$, and $\mathbb{P}^-$.*

Proof. From the previous lemmas we know that $O(m,q)$ acts transitively on $\mathbb{P}_\tau$ for $2\nmid q$, $m\geqslant 2$, and $\tau\in\mathbb{F}_q$. Thus $OZ(m,q)$ acts transitively on $\mathbb{P}^+$, $\mathbb{P}_0$, and $\mathbb{P}^-$. (For $A\in O(m,q)$ and $\alpha\in\mathbb{F}_q^*$ we have $B:=\alpha\cdot A\in OZ(m,q)$ and $\langle Bu,Bu\rangle=\alpha^2\langle u,u\rangle$ for all $u\in\mathbb{F}_q^m$.) □

Lemma 3.18. *Let $u,v\in\mathbb{F}_q^3$ with $u,v\neq 0$. If $\langle u,u\rangle=\langle u,v\rangle=0$ and $\mathbb{F}_q\cdot u\neq\mathbb{F}_q\cdot v$ then we have $\langle v,v\rangle\in\square_q$ if $q\equiv 1 \pmod 4$ and $\langle v,v\rangle\notin\square_q$ if $q\equiv 3 \pmod 4$.*

Proof. If the u_i are non-zero we can assume w.l.o.g. that $u_3=1$. From $\langle u,v\rangle=0$ we conclude $v_3=-v_1u_1-v_2u_2$. Using $u_1^2+u_2^2+1=0$ this results in

$$\begin{aligned}\langle v,v\rangle &= v_1^2+v_2^2+v_1^2u_1^2+v_2^2u_2^2+2v_1v_2u_1u_2\\ &= -u_2^2v_1^2-u_1^2v_2^2+2v_1v_2u_1u_2\\ &= -(u_2v_1-u_1v_2)^2.\end{aligned}$$

As $-1\notin\square_q$ iff $q\equiv 3 \pmod 4$ by Lemma 3.4 we have

$$\langle v,v\rangle\notin\square_q\setminus\{0\} \quad \text{for } q\equiv 3 \pmod 4 \quad \text{and} \quad \langle v,v\rangle\in\square_q \quad \text{for } q\equiv 1 \pmod 4,$$

in this case.

Let us assume $q\equiv 3 \pmod 4$ and $\langle v,v\rangle=0$ for a moment. As $-1\notin\square_q$ we have $u_1,u_2\neq 0$ using $u_1^2+u_2^2+1=0$. Thus we have $v_1=v_2\frac{u_1}{u_2}$. Inserting it yields $v=\left(v_2\frac{u_1}{u_2}\ \ v_2\ \ (-v_2\frac{u_1}{u_2}\cdot u_1-v_2u_2)\right)^T=\frac{v_2}{u_2}\cdot u$. As $u,v\neq 0$ we would have $\mathbb{F}_q\cdot v=\mathbb{F}_q\cdot u$. Thus we even have $\langle v,v\rangle\notin\square_q$ for $q\equiv 3 \pmod 4$.

In the remaining case we assume w.l.o.g. $u_3=0$. As $u_1^2+u_2^2=0$ we have $-1\in\square_q$, $q\equiv 1 \pmod 4$, and $u_1,u_2\neq 0$. We can further assume w.l.o.g. $u_1=1$ and $u_2=\omega_q$, where $\omega_q^2=-1$. With this $\langle u,v\rangle=0$ is equivalent to $v_2=\omega_qv_1$. Thus we have $\langle v,v\rangle=v_3^2\in\square_q$. □

Lemma 3.19. *For $2\nmid q$ and $m\geqslant 3$ the orbits of $\mathbb{F}_q^m$ under the group $\mathrm{Aut}(m,q)\cap GL(m,q)$ are $\mathbb{P}^+$, $\mathbb{P}_0$, and $\mathbb{P}^-$.*

Proof. As $OZ(m,q)\leqslant\mathrm{Aut}(m,q)\cap GL(m,q)$ and due to Lemma 3.17 it may only happen that some elements of $\mathbb{P}^+$, $\mathbb{P}_0$, and $\mathbb{P}^-$ are contained in the same orbit. Due to Definition 3.1 $\mathbb{P}^-$ forms its own orbit. Thus only $\mathbb{P}^+$ and $\mathbb{P}_0$ may be contained in the same orbit. Now we show that this is not the case.

In Section 4 we introduce the graph $\mathfrak{G}_{m,q}$ of integral distances corresponding to $\mathbb{F}_q^m$ and its integral distances. Due to Lemma 4.5 for dimension $m=3$ and $2\nmid q$ the graph $\mathfrak{G}_{3,q}$ is not strongly regular. Thus $\mathbb{P}^+$ and $\mathbb{P}_0$ are disjoint orbits.

For $m\geqslant 4$ let us assume that there exists an element u in $\mathbb{F}_q^m$ with $\langle u,u\rangle=0$ and there exists a matrix A in $\mathrm{Aut}(m,q)\cap GL(m,q)$ with $\langle A^{-1}u,A^{-1}u\rangle\in\square_q\setminus\{0\}$. W.l.o.g. we assume $A^{-1}u=e^{(1)}$, where $e^{(i)}$ is a vector in $\mathbb{F}_q^m$ consisting of zeros and a single one at coordinate i, this is the ith unit vector. So we have $Ae^{(1)}=u$ and we set $w^{(i)}:=Ae^{(i)}\in\mathbb{F}_q^m$, $\mu_i:=\langle u,w^{(i)}\rangle$ for $2\leqslant i\leqslant 4$. Now we show that there exists a vector $v\in\mathbb{F}_q^m$ with $\langle e^{(1)},v\rangle=0$, $\langle v,v\rangle\neq 0$, and $\langle Ae^{(1)},Av\rangle=0$. If there exist $2\leqslant i\leqslant 4$ with $\mu_i=0$ then we may choose $v=e^{(i)}$. Otherwise we have $\mu_2,\mu_3,\mu_4\neq 0$. We remark that $(\frac{\mu_i}{\mu_j})^2=-1$ is equivalent to $(\frac{\mu_j}{\mu_i})^2=-1$ for all $2\leqslant i,j\leqslant 4$. Due to $(\frac{\mu_1}{\mu_2})^2\cdot(\frac{\mu_2}{\mu_3})^2\cdot(\frac{\mu_3}{\mu_1})^2=1\neq -1$ there exist i and j with $i\neq j$, $(\frac{\mu_i}{\mu_j})^2\neq -1$. We set $v:=-\mu_je^{(i)}+\mu_ie^{(j)}$ which yields

$$\langle e^{(1)}, v\rangle = 0, \qquad \langle v, v\rangle = \mu_i^2 + \mu_j^2 \neq 0, \quad \text{and}$$
$$\langle Ae^{(1)}, Av\rangle = \langle u, -\mu_j w^{(i)} + \mu_i w^{(j)}\rangle = -\mu_j\langle u, w^{(i)}\rangle + \mu_i\langle u, w^{(j)}\rangle = 0.$$

Let χ be the characteristic function of $\square_q$, this is $\chi(\alpha) = 1$ for $\alpha \in \square_q$ and $\chi(\alpha) = 0$ for $\alpha \notin \square_q$. We set $\tau := \langle v, v\rangle \neq 0$ and $\nu := \langle Av, Av\rangle$. For all $\lambda_1, \lambda_2 \in \mathbb{F}_q$ we have

$$d^2\big(0, \lambda_1 e^{(1)} + \lambda_2 v\big) = \big\langle \lambda_1 e^{(1)} + \lambda_2 v, \lambda_1 e^{(1)} + \lambda_2 v\big\rangle = \lambda_1^2 + \tau\cdot\lambda_2^2 \quad \text{and}$$
$$d^2\big(0, A\big(\lambda_1 e^{(1)} + \lambda_2 v\big)\big) = \langle \lambda_1 u + \lambda_2 Av, \lambda_1 u + \lambda_2 Av\rangle = \nu\cdot\lambda_2^2.$$

As $A \in \mathrm{Aut}(m,q) \cap GL(m,q)$ we have $\chi(\lambda_1^2 + \tau\cdot\lambda_2^2) = \chi(\nu\cdot\lambda_2^2)$ for all λ_1, λ_2 in $\mathbb{F}_q$. Inserting $\lambda_2 = 1$ yields $\chi(\nu) = \chi(\lambda_1^2 + \tau)$ for all $\lambda_1 \in \mathbb{F}_q$. Due to $|\{\lambda_1^2 + \tau \mid \lambda_1 \in \mathbb{F}_q\}| = \frac{q+1}{2}$ we conclude $\chi(\nu) = \chi(\lambda_1^2 + \tau) = 1$. W.l.o.g. we may assume $\tau = 1 \in \square_q\backslash\{0\}$. Thus for $q = p^r$ and $\alpha \in \square_q$ we have

$$\nu = \chi(\alpha) = \chi(\alpha+1) = \chi\big((\alpha+1)+1\big) = \chi\big((\alpha+2)+1\big) = \cdots = \chi\big((\alpha+p-2)+1\big).$$

We conclude $p \mid |\square_q| = \frac{q+1}{2} = \frac{p^r+1}{2}$, which is a contradiction. □

Lemma 3.20.

$$\mathrm{Aut}(3,q) \cap GL(3,q) = OZ(3,q) \quad \textit{for } 2 \nmid q.$$

Proof. Let $A \in \mathrm{Aut}(3,q) \cap GL(3,q)$ be an automorphism. The idea of the proof is to use the fact that A takes every vector v of integral norm $\langle v, v\rangle \neq 0$ to another vector of integral norm $\neq 0$ with the aim to construct an automorphism in $\mathrm{Aut}(2,q)$. Using the classification of the 2-dimensional automorphisms in Theorem 3.9, see also [17], we conclude $A \in OZ(3,q)$.

Obviously, A is uniquely defined by its images of $e^{(1)} = (1\ 0\ 0)^T$, $e^{(2)} = (0\ 1\ 0)^T$, and $e^{(3)} = (0\ 0\ 1)^T$. Due to Lemmas 3.17 and 3.19 we can assume $A\cdot e^{(1)} = e^{(1)}$. We set $A\cdot e^{(2)} =: (\alpha\ \beta\ \gamma)^T$, where we have

$$\alpha^2 + \beta^2 + \gamma^2 = \nu^2 \in \square_q\backslash\{0\}$$

due to Lemma 3.19. Let $\chi : \mathbb{F}_q \to \{0,1\}$, where $\chi(\tau) = 1$ iff $\tau \in \square_q$, be the characteristic function of $\square_q$. By applying A on $(\lambda\ \mu\ 0)^T$ we obtain

$$\chi\big(\lambda^2 + \mu^2\big) = \chi\big(\lambda^2 + 2\alpha\lambda\mu + \nu^2\mu^2\big) \quad \text{for all } \lambda, \mu \in \mathbb{F}_q. \tag{1}$$

Inserting $\lambda = -2\alpha$, $\mu = 1$ yields $\chi(4\alpha^2 + 1) = \chi(\nu^2) = 1$. Now we prove $\chi(\alpha^2 + 1) = 1$. Putting $\lambda = 2\tau\alpha$, $\mu = 1$ for an arbitrary $\tau \in \mathbb{F}_q$ in Eq. (1) we obtain

$$\chi\big(4\tau^2\alpha^2 + 1\big) = \chi\big(\big(4\tau^2 + 4\tau\big)\alpha^2 + \nu^2\big).$$

Inserting $\lambda = -2(\tau+1)\alpha$, $\mu = 1$ yields

$$\chi\big(4(\tau+1)^2\alpha^2 + 1\big) = \chi\big(\big(4\tau^2 + 4\tau\big)\alpha^2 + \nu^2\big),$$

hence we get

$$\chi\big((2\tau)^2\alpha^2 + 1\big) = \chi\big((2\tau+2)^2\alpha^2 + 1\big)$$

for all $\tau \in \mathbb{F}_q$. For $\tau = 1$ we have $\chi(4\alpha^2 + 1) = 1$, therefore we obtain $\chi((2\tau)^2\alpha^2 + 1) = 1$ for all $\tau \in \mathbb{F}_p$ (but not necessarily for all $\tau \in \mathbb{F}_q$). As we have $p \neq 2$, we can take $\tau = 2^{-1} \in \mathbb{F}_p$ and get $\chi(\alpha^2 + 1) = 1$.

If we insert $\lambda = -\alpha$, $\mu = 1$ in Eq. (1) we obtain

$$1 = \chi\big(\alpha^2 + 1\big) = \chi\big(\lambda^2 + \mu^2\big) = \chi\big(\lambda^2 + 2\alpha\lambda\mu + \nu^2\mu^2\big) = \chi\big(\nu^2 - \alpha^2\big).$$

Thus $\pi \in \mathbb{F}_q$ with $\alpha^2+\pi^2=\nu^2$ exist. Let us consider the matrix $B=\left(\begin{smallmatrix}1 & \alpha\\ 0 & \pi\end{smallmatrix}\right)$. As we have $\chi(\lambda^2+\mu^2)=\chi(\lambda^2+2\alpha\lambda\mu+(\alpha^2+\pi^2)\lambda^2)$ for all $\lambda,\mu\in\mathbb{F}_q$ the matrix B is an automorphism for $\mathbb{F}_q^2$ with respect to Δ.

For $q\neq\{5,9\}$ we can apply Theorem 3.9(3) and conclude $\alpha=0$, $\beta^2+\gamma^2=\pi^2=\nu^2=1$. Now we set $A\cdot e^{(3)}=:\left(\tilde{\alpha}\ \tilde{\beta}\ \tilde{\gamma}\right)^T$ and similarly conclude $\tilde{\alpha}=0$, $\tilde{\beta}^2+\tilde{\gamma}^2=1$. Therefore A has the form

$$A=\begin{pmatrix}1 & 0 & 0\\ 0 & b & \tilde{\beta}\\ 0 & c & \tilde{\gamma}\end{pmatrix}=:\begin{pmatrix}1 & 0 & 0\\ 0 & & \\ 0 & & A'\end{pmatrix}.$$

By applying A to all vectors $(0\ \mu\ \kappa)$ for $\mu,\kappa\in\mathbb{F}_q$ we see that A' is an element of $\mathrm{Aut}(2,q)\cap GL(2,q)$. Due to Theorem 3.9(3) the matrix A' is orthogonal and we conclude $A\in O(3,q)$.

We deal with the missing cases $q\in\{5,9\}$ using the classification of the 2-dimensional automorphism group $\mathrm{Aut}(2,q)$ as follows. Either we use the precise classification in [17] or we use an exhaustive enumeration of the elements in $GL(2,q)$ to conclude $\alpha=0$, $\beta^2+\gamma^2=\pi^2=\nu^2=1$ for $q=5$ and $\alpha=0$, $\beta^2+\gamma^2=\pi^2=\nu^2\in\{\pm1\}$ for $q=9$. Now we set $A\cdot e^{(3)}=:\left(\tilde{\alpha}\ \tilde{\beta}\ \tilde{\gamma}\right)^T$ and similarly conclude $\tilde{\alpha}=0$, $\tilde{\beta}^2+\tilde{\gamma}^2=1$ for $q=5$ and $\tilde{\beta}^2+\tilde{\gamma}^2\in\{\pm1\}$ for $q=9$. Therefore A has the form

$$A=\begin{pmatrix}1 & 0 & 0\\ 0 & b & \tilde{\beta}\\ 0 & c & \tilde{\gamma}\end{pmatrix}=:\begin{pmatrix}1 & 0 & 0\\ 0 & & \\ 0 & & A'\end{pmatrix}.$$

Additionally we have $\langle Ae^{(2)},Ae^{(3)}\rangle=0$ in both cases, where we refer to [17] or an exhaustive enumeration. Next we exclude the case $\beta^2+\gamma^2=-1$ for $q=9$. We use $\mathbb{F}_9\simeq\mathbb{F}_3[x]/(x^2+1)$ and assume the contrary $\beta^2+\gamma^2=-1$. As A is an automorphism of $\mathbb{F}_9^3$ with respect to Δ we have

$$\chi\left(\lambda^2+\mu^2+\kappa^2\right)=\chi\left(\lambda^2+(\beta\mu+\tilde{\beta}\kappa)^2+(\gamma\mu+\tilde{\gamma}\kappa)^2\right)=\chi\left(\lambda^2+\left(\beta^2+\gamma^2\right)\mu^2+\left(\tilde{\beta}^2+\tilde{\gamma}^2\right)\kappa^2\right)$$

for all $\lambda,\mu,\kappa\in\mathbb{F}_9$. Inserting $\lambda=1$, $\mu=1$, and $\kappa=x+2$ yields

$$\chi\left(\lambda^2+\mu^2+\kappa^2\right)=\chi\left(2+x^2+4x+4\right)=\chi(x+2)=0$$

and

$$\chi\left(\lambda^2+\left(\beta^2+\gamma^2\right)\mu^2+\left(\tilde{\beta}^2+\tilde{\gamma}^2\right)\kappa^2\right)=\chi\left(\left(\tilde{\beta}^2+\tilde{\gamma}^2\right)\kappa^2\right)=1,$$

a contradiction. Thus due to symmetry we have $\beta^2+\gamma^2=\tilde{\beta}^2+\tilde{\gamma}^2=1$ and $A\in O(3,q)$ in both cases. □

Proof of Theorem 3.2. We prove the theorem by induction on the dimension m. For the induction basis we refer to Lemma 3.20. Now let $m\geqslant 4$ and $A\in\mathrm{Aut}(m,q)\cap GL(m,q)$ be an automorphism. Due to Lemmas 3.17 and 3.19 we can assume $A\cdot e^{(1)}=e^{(1)}$, where $e^{(i)}=\left(0\cdots0\ \underbrace{1}_{i\text{th position}}\ 0\cdots0\right)^T$ again denotes the ith unit vector. For $2\leqslant i\leqslant m$ we set $A\cdot e^{(i)}=:(\nu_{1,i}\ \cdots\ \nu_{m,i})^T$, where we have

$$\sum_{j=1}^{m}\nu_{j,i}^2=\nu_i^2\in\square_q\backslash\{0\}.$$

Using a similar calculation as in the proof of Lemma 3.20 we obtain $\nu_{1,i}=0$ and $\sum_{j=1}^{m}\nu_{j,i}^2=1$ for all $2\leqslant i\leqslant m$. Therefore A has the form

$$A=\begin{pmatrix}1 & 0 & 0 & \cdots\\ 0 & \nu_{1,2} & \nu_{1,3} & \cdots\\ 0 & \nu_{2,2} & \nu_{2,3} & \cdots\\ \vdots & \vdots & \vdots & \ddots\end{pmatrix}=:\begin{pmatrix}1 & 0 & \cdots\\ 0 & & \\ \vdots & & A'\end{pmatrix}.$$

As A is an automorphism of $\mathbb{F}_q^m$ with respect to Δ the matrix A' is an automorphism of $\mathbb{F}_q^{m-1}$ with respect to Δ. Due to $\sum_{j=1}^m v_{j,i}^2 = 1$ for all $2 \leqslant i \leqslant m$ and the induction hypothesis we have $A' \in O(m-1,q)$. Thus we have $A \in O(m,q)$. □

4. Graph of integral distances

It turns out that it is useful to model integral point sets as cliques of certain graphs. For a given prime power $q = p^r$ and a given dimension m we define a graph $\mathfrak{G}_{m,q}$ with vertex set $\mathbb{F}_q^m$, where two vertices u and v are adjacent if $d^2(u,v) \in \square_q$. In this section we want to study the properties of $\mathfrak{G}_{m,q}$. A motivation for this study is that the graph $\mathfrak{G}_{2,q}$ for dimension $m = 2$ is a strongly regular graph. A graph is strongly regular, if there exist positive integers k, λ, and μ such that every vertex has k neighbors, every adjacent pair of vertices has λ common neighbors, and every nonadjacent pair has μ common neighbors, see e.g. [24]. If we denote the number of vertices by v, our graph $\mathfrak{G}_{2,q}$ has the parameters

$$(v,k,\lambda,\mu) = \left(q^2, \frac{(q-1)(q+3)}{2}, \frac{(q+1)(q+3)}{4} - 3, \frac{(q+1)(q+3)}{4}\right) \quad \text{for } q \equiv 1 \pmod 4,$$

and the parameters

$$(v,k,\lambda,\mu) = \left(q^2, \frac{q^2-1}{2}, \frac{q^2-1}{4} - 1, \frac{q^2-1}{4}\right) \quad \text{for } q \equiv 3 \pmod 4.$$

See e.g. [11] for this fact, which is easy to prove.

For $2 \mid q$ or $m = 1$ the graph of integral distances $\mathfrak{G}_{m,q}$ is equivalent to a complete graph on q^m vertices. Thus we assume $2 \nmid q$ and $m \geqslant 3$ in the following.

As the translations of $\mathbb{F}_q^m$ are automorphisms with respect to Δ acting transitively on the points we know that $\mathfrak{G}_{m,q}$ is a regular graph, which means that every vertex u has an equal number of neighbors, called the degree of u. Thus we can speak of a degree of $\mathfrak{G}_{m,q}$.

Lemma 4.1. *The degree of $\mathfrak{G}_{3,q}$ is given by*

$$\mathcal{D}(3,q) = \begin{cases} (q-1)\cdot\frac{(q+2)(q+1)}{2} & \text{if } q \equiv 1 \pmod 4, \\ (q-1)\cdot\frac{q^2+q+2}{2} & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Proof. It suffices to determine the number of vectors $(\alpha\ \beta\ \gamma)^T \neq 0$ fulfilling $\alpha^2+\beta^2+\gamma^2 \in \square_q$. So let $\alpha^2+\beta^2+\gamma^2 = \nu^2$. If $\nu = 0$ then we have $\alpha^2+\beta^2 = -\gamma^2$. Using Corollary 3.7 we obtain q^2-1 solutions in this case. For $\nu \neq 0$ we have $\frac{q-1}{2}$ possible values for ν^2. Using Corollary 3.7 we obtain the number of solutions (α,β) of the equation $\alpha^2+\beta^2 = \nu^2-\gamma^2$ for all possible values of γ and ν. Summing up everything yields the stated formula. □

To determine the degree $\mathcal{D}(m,q)$ of the graph of integral distances $\mathfrak{G}_{m,q}$ in arbitrary dimension we define the three functions

$$\mathcal{S}(m,q) := \left|\left\{u \in \mathbb{F}_q^m \;\middle|\; \sum_{i=1}^m u_i^2 \in \square_q \backslash \{0\}\right\}\right|, \qquad \mathcal{Z}(m,q) := \left|\left\{u \in \mathbb{F}_q^m \;\middle|\; \sum_{i=1}^m u_i^2 = 0\right\}\right|, \quad \text{and}$$

$$\mathcal{N}(m,q) := \left|\left\{u \in \mathbb{F}_q^m \;\middle|\; \sum_{i=1}^m u_i^2 \notin \square_q\right\}\right|.$$

We would like to remark that $\mathcal{S}(m,q) = |\mathbb{P}^+|$ and $\mathcal{N}(m,q) = |\mathbb{P}^-|$, where $\mathbb{P}^+$ and $\mathbb{P}^-$ denote the sets of Definition 3.16. The first few functions are given by

$$\mathcal{S}(1,q)=q-1,\qquad \mathcal{Z}(1,q)=1,\qquad \mathcal{N}(1,q)=0,$$
$$\mathcal{S}(2,q)=\begin{cases}\frac{(q-1)^2}{2} & \text{if } q\equiv 1 \pmod 4,\\ \frac{q^2-1}{2} & \text{if } q\equiv 3 \pmod 4,\end{cases}$$
$$\mathcal{Z}(2,q)=\begin{cases}2q-1 & \text{if } q\equiv 1 \pmod 4,\\ 1 & \text{if } q\equiv 3 \pmod 4,\end{cases}\quad \text{and}$$
$$\mathcal{N}(2,q)=\begin{cases}\frac{(q-1)^2}{2} & \text{if } q\equiv 1 \pmod 4,\\ \frac{q^2-1}{2} & \text{if } q\equiv 3 \pmod 4,\end{cases}$$

see Corollary 3.7. To determine these functions recursively we can use:

Lemma 4.2. *Let $\mathbb{I}_0$ and $\mathbb{I}_1$ be the sets defined in Corollary* 3.7. *Then for dimension $m\geqslant 3$ we have*

$$\mathcal{Z}(m,q)=\mathcal{Z}(m-2,q)\cdot|\mathbb{I}_0|+\big(q^{m-2}-\mathcal{Z}(m-2,q)\big)\cdot|\mathbb{I}_1|,$$
$$\mathcal{S}(m,q)=\frac{q-1}{2}\cdot\big(\mathcal{N}(m-2,q)+\mathcal{Z}(m-2,q)\big)\cdot|\mathbb{I}_1|+\frac{q-3}{2}\cdot\mathcal{S}(m-2,q)\cdot|\mathbb{I}_1|+\mathcal{S}(m-2,q)\cdot|\mathbb{I}_0|,$$
$$\mathcal{N}(m,q)=q^m-\mathcal{S}(m,q)-\mathcal{Z}(m,q),\quad \textit{and}$$
$$\mathcal{D}(m,q)=\mathcal{S}(m,q)+\mathcal{Z}(m,q)-1.$$

Proof. We rewrite the equation $\sum_{i=1}^m u_i^2=\tau$ as $u_1^2+u_2^2=\tau-\sum_{i=3}^m u_i^2$ and apply Corollary 3.7. □

Theorem 4.3. *Let $m\geqslant 1$ be arbitrary. For $q\equiv 1 \pmod 4$ we have*

$$\mathcal{Z}(m,q)=\begin{cases}q^{m-1} & \textit{for } m \textit{ odd},\\ q^{m-1}+q^{\frac{m}{2}}-q^{\frac{m-2}{2}} & \textit{for } m \textit{ even},\end{cases}$$
$$\mathcal{S}(m,q)=\begin{cases}\frac{1}{2}(q^m-q^{m-1}+q^{\frac{m+1}{2}}-q^{\frac{m-1}{2}}) & \textit{for } m \textit{ odd},\\ \frac{1}{2}(q^m-q^{m-1}-q^{\frac{m}{2}}+q^{\frac{m-2}{2}}) & \textit{for } m \textit{ even},\end{cases}$$
$$\mathcal{N}(m,q)=\begin{cases}\frac{1}{2}(q^m-q^{m-1}-q^{\frac{m+1}{2}}+q^{\frac{m-1}{2}}) & \textit{for } m \textit{ odd},\\ \frac{1}{2}(q^m-q^{m-1}-q^{\frac{m}{2}}+q^{\frac{m-2}{2}}) & \textit{for } m \textit{ even},\end{cases}$$
$$\mathcal{D}(m,q)=\begin{cases}\frac{1}{2}(q^m+q^{m-1}+q^{\frac{m+1}{2}}-q^{\frac{m-1}{2}})-1 & \textit{for } m \textit{ odd},\\ \frac{1}{2}(q^m+q^{m-1}+q^{\frac{m}{2}}-q^{\frac{m-2}{2}})-1 & \textit{for } m \textit{ even}.\end{cases}$$

For $q\equiv 3 \pmod 4$ we have

$$\mathcal{Z}(m,q)=\begin{cases}q^{m-1} & \textit{for } m \textit{ odd},\\ q^{m-1}+(-q)^{\frac{m}{2}}+(-q)^{\frac{m-2}{2}} & \textit{for } m \textit{ even},\end{cases}$$
$$\mathcal{S}(m,q)=\begin{cases}\frac{1}{2}(q^m-q^{m-1}-(-q)^{\frac{m+1}{2}}-(-q)^{\frac{m-1}{2}}) & \textit{for } m \textit{ odd},\\ \frac{1}{2}(q^m-q^{m-1}-(-q)^{\frac{m}{2}}-(-q)^{\frac{m-2}{2}}) & \textit{for } m \textit{ even},\end{cases}$$
$$\mathcal{N}(m,q)=\begin{cases}\frac{1}{2}(q^m-q^{m-1}+(-q)^{\frac{m+1}{2}}+(-q)^{\frac{m-1}{2}}) & \textit{for } m \textit{ odd},\\ \frac{1}{2}(q^m-q^{m-1}-(-q)^{\frac{m}{2}}-(-q)^{\frac{m-2}{2}}) & \textit{for } m \textit{ even},\end{cases}$$

$$\mathcal{D}(m,q)=\begin{cases}\frac{1}{2}(q^m+q^{m-1}-(-q)^{\frac{m+1}{2}}-(-q)^{\frac{m-1}{2}})-1 & \text{for } m \text{ odd},\\ \frac{1}{2}(q^m+q^{m-1}+(-q)^{\frac{m}{2}}+(-q)^{\frac{m-2}{2}})-1 & \text{for } m \text{ even}.\end{cases}$$

Proof. Induction on m using Lemma 4.2. □

With strongly regular graphs in mind we consider the number of common neighbors.

Theorem 4.4. *If $\mathcal{A}(m,q)$ denotes the number of common neighbors of 0 and $e^{(1)}=(1\,0\cdots 0)^T$ in $\mathbb{F}_q^m\backslash\{0,e^{(1)}\}$, then for $m\geqslant 1$ we have*

$$\mathcal{A}(m,q)=\begin{cases}\frac{q^{m-2}\cdot(q+1)^2+(-1)^{\frac{(m-1)(q-1)}{4}}\cdot q^{\frac{m-3}{2}}\cdot(3q^2-2q-1)}{4}-2 & \text{for } m \text{ odd},\\ \frac{q^{m-2}\cdot(q+1)^2+2\cdot(-1)^{\frac{m(q-1)}{4}}\cdot q^{\frac{m-2}{2}}\cdot(q-1)}{4}-2 & \text{for } m \text{ even}.\end{cases}$$

Proof. Clearly we have $\mathcal{A}(1,q)=q-2$. For $m\geqslant 1$ we count the number of solutions $(v_1,\ldots,v_m)$ of the equation system

$$v_1^2+\sum_{i=2}^{m}v_i^2=\alpha^2,\qquad (v_1-1)^2+\sum_{i=2}^{m}v_i^2=\beta^2.$$

There are $(\frac{q+1}{2})^2$ different pairs (α^2,β^2) for $\alpha,\beta\in\mathbb{F}_q$. For given α^2,β^2 we have $v_1=\frac{\alpha^2-\beta^2+1}{2}$ and $\sum_{i=2}^{m}v_i^2=\frac{4\alpha^2\beta^2-(\alpha^2+\beta^2-1)^2}{4}=-(\frac{\alpha^2-\beta^2-1}{2})^2+\beta^2=:\tau$. Each of the $(\frac{q+1}{2})^2$ cases leads to a specific $\tau\in\mathbb{F}_q$. Now let a_ν be the number of pairs (α^2,β^2) which result in $\tau=\nu$. Then we obtain

$$\sum_{\nu\in\mathbb{F}_q}a_\nu=\left(\frac{q+1}{2}\right)^2. \tag{2}$$

By $b_{m,\nu}$ we denote the number of vectors $(v_2\ \cdots\ v_m)\in\mathbb{F}_q^{m-1}$ with $\sum_{j=2}^{m}v_j^2=\nu$. With this we have

$$\mathcal{A}(m,q)=\sum_{\nu\in\mathbb{F}_q}a_\nu\cdot b_{m,\nu}-2. \tag{3}$$

Due to $\mathcal{A}(1,q)=q-2$ and $b_{1,\nu}=0$ for $\nu\neq 0$ we have $a_0=q$. If $\nu,\mu\in\square_q\backslash\{0\}$ or $\nu,\mu\notin\square_q$ then we have $b_{m,\nu}=b_{m,\mu}$. Next we show

$$a_+:=\sum_{\nu\in\square_q\backslash\{0\}}a_\nu=\begin{cases}\frac{(q+1)(q-1)}{8} & \text{for } q\equiv 1 \bmod 4\\ \frac{(q-1)(q-3)}{8} & \text{for } q\equiv 3 \bmod 4,\end{cases} \tag{4}$$

from which we can conclude

$$a_-:=\sum_{\nu\notin\square_q}a_\nu=\begin{cases}\frac{(q-1)(q-3)}{8} & \text{for } q\equiv 1 \bmod 4\\ \frac{(q+1)(q-1)}{8} & \text{for } q\equiv 3 \bmod 4,\end{cases}$$

due to Eq. (2). We use the information for dimension $m=2$. For $\nu\notin\square_q$ we have $b_{2,\nu}=0$ and for $\nu\in\square_q\backslash\{0\}$ we have $b_{2,\nu}=2$. For $q\equiv 3 \pmod 4$ we have $b_{2,0}=1$ and for $q\equiv 1 \pmod 4$ we have $b_{2,0}=1$. Inserting this and the formula for $\mathcal{A}(2,q)$ in Eq. (3) yields Eq. (4).

Using $b_{m,0}=\mathcal{Z}(m-1,q)$, $b_{m,\nu}=\frac{2}{q-1}\cdot\mathcal{S}(m-1,q)$ for $\nu\in\square_q\backslash\{0\}$, and $b_{m,\nu}=\frac{2}{q-1}\cdot\mathcal{N}(m-1,q)$ for $\nu\notin\square_q$ we get

$$\mathcal{A}(m,q)=q\cdot\mathcal{Z}(m-1,q)+a_+\cdot\frac{2}{q-1}\cdot\mathcal{S}(m-1,q)+a_-\cdot\frac{2}{q-1}\cdot\mathcal{N}(m-1,q)-2$$

and we obtain the stated formula by using Theorem 4.3. □

So for dimension $m = 3$ we have $\mathcal{A}(3,q) = \frac{q^3+5q^2-q-9}{4}$ for $q \equiv 1 \pmod 4$ and $\mathcal{A}(3,q) = \frac{q^3-q^2+3q-7}{4}$ for $q \equiv 3 \pmod 4$.

Lemma 4.5. *For odd dimension $m \geqslant 3$ the graph of integral distances $\mathfrak{G}_{m,q}$ is not a strongly regular graph.*

Proof. Let us assume that $\mathfrak{G}_{m,q}$ is strongly regular. Then there exist corresponding parameters (v,k,λ,μ) with

$$v = q^m, \qquad k = \mathcal{D}(m,q), \quad \text{and} \quad \lambda = \mathcal{A}(m,q).$$

For a strongly connected graph we have the identity $(v-k-1)\mu = k(k-\lambda-1)$, see e.g. [24]. Using Theorems 4.3 and 4.4 we can use this identity to determine μ. For $q \equiv 1 \pmod 4$ and m odd we have

$$k(k-\lambda-1) = \frac{q^{\frac{m-3}{2}}(q-1)(q+1)(q^{\frac{m-1}{2}}-1)(q^m+q^{m-1}+q^{\frac{m+1}{2}}-q^{\frac{m-1}{2}}-2)}{8},$$
$$v-k-1 = \frac{q^{\frac{m-1}{2}}\cdot(q-1)\cdot(q^{\frac{m-1}{2}}-1)}{2}, \quad \text{and}$$
$$\mu = \frac{(q+1)\cdot(q^m+q^{m-1}+q^{\frac{m+1}{2}}-q^{\frac{m-1}{2}}-2)}{4q}.$$

For $q \equiv 3 \pmod 4$ and m odd we obtain

$$k(k-\lambda-1) = \frac{q^{\frac{m-3}{2}}(q-1)(q+1)(q^{\frac{m-1}{2}}-(-1)^{\frac{m-1}{2}})}{8}\cdot\left(q^m+q^{m-1}-(-q)^{\frac{m+1}{2}}-(-q)^{\frac{m-1}{2}}-2\right),$$
$$v-k-1 = \frac{q^{\frac{m-1}{2}}\cdot(q-1)\cdot(q^{\frac{m-1}{2}}-(-1)^{\frac{m-1}{2}})}{2}, \quad \text{and}$$
$$\mu = \frac{(q+1)\cdot(q^m+q^{m-1}-(-q)^{\frac{m+1}{2}}-(-q)^{\frac{m-1}{2}}-2)}{4q}.$$

As for odd $m \geqslant 3$ the denominator of μ is divisible by q and the numerator is not divisible by q, the graph of integral distances $\mathfrak{G}_{m,q}$ is not a strongly regular graph in these cases. □

If we accomplish the same computation for even m then for $q \equiv 1 \pmod 4$ we get

$$k(k-\lambda-1) = \frac{q^{m-2}\cdot(q-1)\cdot(q+1)\cdot(q^{\frac{m}{2}}-1)\cdot(q^{\frac{m}{2}}+q^{\frac{m-2}{2}}+2)}{8},$$
$$v-k-1 = \frac{q^{\frac{m-2}{2}}\cdot(q-1)\cdot(q^{\frac{m}{2}}-1)}{2}, \quad \text{and}$$
$$\mu = \frac{q^{\frac{m-2}{2}}\cdot(q+1)\cdot(q^{\frac{m}{2}}+q^{\frac{m-2}{2}}+2)}{4},$$

and for $q \equiv 3 \pmod 4$ we obtain

$$k(k-\lambda-1) = \frac{q^{m-2}(q-1)(q+1)(q^{\frac{m}{2}}-(-1)^{\frac{m}{2}})(q^{\frac{m}{2}}+q^{\frac{m-2}{2}}+2\cdot(-1)^{\frac{m}{2}})}{8},$$
$$v-k-1 = \frac{q^{\frac{m-2}{2}}\cdot(q-1)\cdot(q^{\frac{m}{2}}-(-1)^{\frac{m}{2}})}{2}, \quad \text{and}$$
$$\mu = \frac{q^{\frac{m-2}{2}}\cdot(q+1)\cdot(q^{\frac{m}{2}}+q^{\frac{m-2}{2}}+2\cdot(-1)^{\frac{m}{2}})}{4}.$$

So in both cases we have $\mu \in \mathbb{N}$ for even dimension m. Therefore the graph $\mathfrak{G}_{m,q}$ could be strongly regular for even dimension m, and indeed this is our conjecture:

Conjecture 4.6. *If $\mathcal{B}(m,q)$ denotes the number of common neighbors of 0 and an element v with $\langle v,v\rangle = 0$ in $\mathbb{F}_q^m \setminus \{0, v\}$, then for $m \geqslant 2$ we have*

$$\mathcal{B}(m,q) = \begin{cases} \mathcal{A}(m,q) & \text{for } m \text{ even}, \\ \mathcal{A}(m,q) - (-1)^{\frac{(q-1)(m-1)}{4}} \cdot q^{\frac{m-3}{2}} \cdot \frac{q^2-1}{4} & \text{for } m \text{ odd}. \end{cases}$$

For even dimension m the graph of integral distances $\mathfrak{G}_{m,q}$ is a strongly regular graph.

We remark that due to Lemma 3.19 $\mathcal{B}(m,q)$ is well defined. For $q = p^1$ being a prime we have verified Conjecture 4.6 for small values using computer calculations. More explicitly, Conjecture 4.6 is valid for $(m = 3,\ p \leqslant 2029)$, $(m = 4,\ p \leqslant 283)$, $(m = 5,\ p \leqslant 97)$, $(m = 6,\ p \leqslant 59)$, $(m = 7,\ p \leqslant 31)$, and $(m = 8,\ p \leqslant 23)$.

5. Maximum cardinality of integral point sets in $\mathbb{F}_q^m$

In Section 2 we have introduced the notion $\mathcal{I}(m,q)$ for the maximum cardinality of an integral point set over $\mathbb{F}_q^m$. As for $m = 1$ or $2 \mid q$ all distances in $\mathbb{F}_q^m$ are integral, we have $\mathcal{I}(m,q) = q^m$ in these cases. We have already stated $\mathcal{I}(2,q) = q$ for $2 \nmid q$ in Theorem 2.3. Combining this with the obvious bound $\mathcal{I}(m,q) \leqslant q \cdot \mathcal{I}(m-1,q)$ we obtain

$$\mathcal{I}(3,q) \leqslant q^2$$

for $2 \nmid q$ and the next open case of dimension $m = 3$.

Theorem 5.1. *If $q \equiv 1 \pmod 4$ then we have $\mathcal{I}(3,q) = q^2$.*

Proof. Consider the point set

$$\mathbb{P} := \left\{ (\alpha, \omega_q \alpha, \beta) \;\middle|\; \alpha, \beta \in \mathbb{F}_q \right\}.$$

This point set is an integral point set of cardinality q^2. □

We remark that the constructed point set geometrically is a hyperplane of $\mathbb{F}_q^3$.

Using the graph of integral distances $\mathfrak{G}_{m,q}$ from Section 4 the problem of determining $\mathcal{I}(m,q)$ is transferred to the well-known problem of the determination of the maximum cardinality of cliques, these are complete subgraphs, in $\mathfrak{G}_{m,q}$. For the latter problem software packages as e.g. Cliquer [20] are available.

Thus for small values m and q the maximum cardinality $\mathcal{I}(m,q)$ can be exactly determined using computer calculations. In the remaining part of this section we will deal with the cases $q \nmid 2$, $m \geqslant 3$. As $\mathfrak{G}_{m,q}$ consists of q^m vertices one should reduce the problem whenever possible. One possibility is to prescribe points that must be contained in the clique. Due to Lemma 3.19 it suffices to investigate the two cases where we prescribe $0 \in \mathbb{F}_q^m$ and an arbitrary element of $\mathbb{P}^+$ or $\mathbb{P}_0$.

Let us consider the special case of dimension $m = 3$ and $q \equiv 3 \pmod 4$. Due to $\mathcal{I}(m,q) \geqslant q$ we can restrict our search on cliques $\mathbb{D}$ with cardinality at least $q+1$. Thus there exists $\gamma \in \mathbb{F}_q$ such that the hyperplane $\{(\alpha\ \beta\ \gamma)^T \mid \alpha, \beta \in \mathbb{F}_q\}$ contains at least two points of a clique $\mathbb{D}$ with cardinality at least $q+1$. We assume $\gamma = 0$ and as for $q \equiv 3 \pmod 4$ the equation $\alpha^2 + \beta^2 = 0$ has the unique solution $\alpha = \beta = 0$ w.l.o.g. we prescribe the points $(0\ 0\ 0)^T$ and $(1\ 0\ 0)^T$. Additionally we know the following: Either in such a clique $\mathbb{D}$ there exists a third point in the hyperplane with third coordinate being equal to zero, or there exist two points in a hyperplane with third coordinate being equal to an element of $\mathbb{F}_q^*$, or every hyperplane with fix third coordinate contains at least one element of the clique $\mathbb{D}$. Using theses properties we were able to determine the following values of $\mathcal{I}(3,q)$ for small q:

q	3	5	7	11	13	17	19	23	27	29	31	37	41
$\mathcal{I}(3,q)$	4	25	8	11	169	289	19	23	28	841	31	1369	1681

For any given point $u \in \mathbb{F}_q^3 \backslash \{0\}$ the point set $u \cdot \mathbb{F}_q$ is an integral point set over $\mathbb{F}_q^3$ of cardinality q. For $q \equiv 3 \pmod 4$ there is another nice construction of an integral point set in $\mathbb{F}_q^3$ with cardinality q. Firstly we construct an integral point set *on a circle*, see [11]. Therefore we consider the field $\mathbb{F}'_q := \mathbb{F}_q[x]/(x^2+1)$. For $\zeta = \alpha + \beta x \in \mathbb{F}'_q$ with $\alpha, \beta \in \mathbb{F}_q$ we set $\overline{\zeta} := \alpha - \beta x \in \mathbb{F}'_q$, which mimics the complex conjugation. Now let ζ be a generator of the cyclic group $\mathbb{F}'_q \backslash \{0\}$. We define $\mathbb{D}' := \{\zeta \in \mathbb{F}'_q \mid \zeta\overline{\zeta} = 1\}$. It is not difficult to check that $\mathbb{D}'$ corresponds to an integral point set over $\mathbb{F}_q^2$ of cardinality $\frac{q+1}{2}$, see [11]. By $\mathbb{D}$ we denote the corresponding integral point set over $\mathbb{F}_q^3$, where the third coordinates of the points are equal to zero. Now we define the set $\mathbb{L} := \{\tau \mid \tau^2 + 1 \in \square_q\}$ which has cardinality $\frac{q-1}{2}$ for $q \equiv 3 \pmod 4$. With this notation we can state:

Lemma 5.2. *For $q \equiv 3 \bmod 4$ the set $\mathbb{D} \cup (0\ 0\ 1) \cdot \mathbb{L}$ is an integral point set over $\mathbb{F}_q^3$ with cardinality q.*

Lemma 5.3. *For $q \equiv 3 \pmod 4$ there exists a hyperplane $\mathbb{H}$ with squared distances being either 0 or non-squares.*

Proof. Due to Corollary 3.7 there exist $\alpha, \beta \in \mathbb{F}_q$ with $\alpha^2 + \beta^2 = -1$. We set $u := (\alpha\ \beta\ 1)^T$ and $v := (-\beta\ \alpha\ 0)^T$. This yields $\langle u, u\rangle = 0$, $\langle v, v\rangle = -1 \notin \square_q$, and $\langle u, v\rangle = 0$. Now let $\mathbb{H} := \{\tau u + \nu v \mid \tau, \nu \in \mathbb{F}_q\}$. The squared distance of two elements $\tau_i u + \nu_i v \in \mathbb{H}$, $i = 1, 2$, is given by $(\nu_1 - \nu_2)^2 \cdot \langle v, v\rangle \notin \square_q \backslash \{0\}$. □

Corollary 5.4. *Let $\mathbb{P}$ be an integral point set in $\mathbb{F}_q^3$ for $q \equiv 3 \pmod 4$. Either $|\mathbb{P}| \leqslant q$ or some squared distances are equal to zero.*

Proof. We consider a covering of $\mathbb{F}_q^3$ by q translations of the plane of Lemma 5.3. □

We remark that our two examples of integral point sets of cardinality q for $q \equiv 3 \pmod 4$ do not contain a squared distance being equal to zero.

As for $q \equiv 3 \pmod 4$ integral point sets over $\mathbb{F}_q^3$ of cardinality $q+1$ seem to be something special we want to list the examples that we have found by our clique search. For $q = 3$ we have

$$\big\{(0,0,0), (1,0,0), (2,1,1), (2,2,1)\big\}$$

and for $q = 7$ we have

$$\big\{(0,0,0), (1,0,0), (0,0,1), (1,5,5), (2,1,3), (3,1,2), (5,5,1), (6,3,6)\big\}$$

as examples. For $\mathcal{I}(3,27) = 28$ an example is given by

$$\begin{aligned}\big\{&\big(2+2w+2w^2, 2+w^2, w^2\big), \big(0, 2w+2w^2, 1+2w\big), \big(1, 1+w+w^2, w\big), (2,0,0),\\ &\big(2, w^2, 2+w\big), \big(2, 2w^2, 1+2w\big), \big(2, 2w+2w^2, 1+2w\big), \big(w, 2+2w, 2+2w+2w^2\big),\\ &\big(2w, 2w^2, 2+2w+w^2\big), \big(2+2w, w^2, 2+w+w^2\big), \big(2+2w, w+2w^2, w+2w^2\big),\\ &\big(2+2w, 2w+2w^2, 2w\big), \big(w^2, 2+w+w^2, 1+2w^2\big), \big(1+w^2, 2w+2w^2, 2w\big), (0,0,0),\\ &\big(2+w^2, 1+2w, 2w^2\big), \big(1+w+w^2, w^2, 2+w^2\big), \big(2+w+w^2, w^2, 0\big), (1,0,0),\\ &\big(2w+w^2, 1+2w+2w^2, 2+2w+2w^2\big), \big(2+2w+w^2, 2+2w^2, 1\big),\\ &\big(1,0,1+w^2\big), \big(1+2w^2, w+w^2, 2w\big), \big(w+2w^2, 1+w^2, 1+w+2w^2\big),\\ &\big(2+w+2w^2, 2+w, 2+w+2w^2\big), \big(2+w+2w^2, 2+2w, 2w+w^2\big),\\ &\big(1+2w+2w^2, 2+w+w^2, 2w+w^2\big), \big(1+2w+2w^2, 2w+2w^2, 2w\big)\big\},\end{aligned}$$

where we use $\mathbb{F}_{27} \simeq \mathbb{F}_3[w]/(w^3+w^2+w+2)$.

For higher dimensions we know some more exact numbers, see [13,14]: $\mathcal{I}(4,3)=9$, $\mathcal{I}(5,3)=27$, $\mathcal{I}(6,3)=33$, $\mathcal{I}(4,5)=25$, $\mathcal{I}(5,5)=125$, $\mathcal{I}(4,7)=49$, $\mathcal{I}(5,7)=343$, and $\mathcal{I}(4,11)=121$.

To obtain lower bounds we can consider pairs of integral point sets $\mathbb{P}_1 \subset \mathbb{F}_q^{m_1}$ and $\mathbb{P}_2 \subset \mathbb{F}_q^{m_2}$, where all squared distances in $\mathbb{P}_2$ are equal to zero. An integral point set of cardinality $|\mathbb{P}_1| \cdot |\mathbb{P}_2|$ in $\mathbb{F}_q^{m_1+m_2}$ is given by $\{\binom{u}{v} \mid u \in \mathbb{P}_1,\ v \in \mathbb{P}_2\}$.

Theorem 5.5. *For $q \equiv 1 \pmod 4$, $m \geqslant 1$, and $2n \leqslant m$ we have*

$$\mathcal{I}(m,q) \geqslant q^n \cdot \mathcal{I}(m-2n,q) \geqslant q^{\lceil \frac{m}{2} \rceil},$$

where we set $\mathcal{I}(0,q)=1$.

Proof. We set $\mathbb{P}_2 := \{(\alpha_1\ \alpha_1\omega_q\ \cdots\ \alpha_n\ \alpha_n\omega_q)^T \mid \alpha_1,\ldots,\alpha_n \in \mathbb{F}_q\}$ in the above described construction. Thus we have $\mathcal{I}(m,q) \geqslant q^n \cdot \mathcal{I}(m-2n,q)$ for all $2n \leqslant m$. The remaining inequality can be proven by induction on m using $\mathcal{I}(m,q) \geqslant q$. □

We would like to remark that the lower bound of Theorem 5.5 is sharp for $m \leqslant 3$ and $q=5$, $m \leqslant 5$.

Lemma 5.6. *There exists an integral point set $\mathbb{P}_2$ in $\mathbb{F}_q^4$ of cardinality q^2, where all squared distances are equal to zero.*

Proof. Let (α,β) be a solution of $\alpha^2+\beta^2=-2$ in $\mathbb{F}_q$. By Corollary 3.7 there are at least $q-1 \geqslant 1$ such solutions. We consider the vectors $u=(\alpha\ \beta\ 1\ 1)^T$ and $v=(-\beta\ \alpha\ -1\ 1)^T$. Obviously u and v are linearly independent and fulfill $\langle u,v\rangle=0$, $\langle u,u\rangle=0$, and $\langle v,v\rangle=0$. We set $\mathbb{P}_2 := \{\tau u+\nu v \mid \tau,\nu \in \mathbb{F}_q\}$. It suffices to check $d^2(0,\tau u+\nu v)=0$ for all $\tau,\nu \in \mathbb{F}_q$. Indeed we have

$$d^2(0,\tau u+\nu v) = \langle \tau u+\nu v, \tau u+\nu v\rangle = \tau^2\langle u,u\rangle + 2\tau\nu\langle u,v\rangle + \nu^2\langle v,v\rangle = 0. \qquad \square$$

Theorem 5.7. *For $q \equiv 3 \pmod 4$, $m \geqslant 1$, and $4n \leqslant m$ we have*

$$\mathcal{I}(m,q) \geqslant q^{2n} \cdot \mathcal{I}(m-4n,q) \geqslant q^{2\cdot\lfloor \frac{m}{4} \rfloor + \lceil \frac{m}{4} - \lfloor \frac{m}{4} \rfloor \rceil} \geqslant q^{\lfloor \frac{m}{2} \rfloor},$$

where we set $\mathcal{I}(0,q)=1$.

Proof. We choose $\mathbb{P}_2$ as the n-fold cartesian product from the integral point set of Lemma 5.6 in the construction described above Lemma 5.5. Thus we have $\mathcal{I}(m,q) \geqslant q^{2n} \cdot \mathcal{I}(m-4n,q)$ for all $2n \leqslant m$. The remaining inequality can by proven by induction on m using $\mathcal{I}(m,q) \geqslant q$. □

The lower bound of Theorem 5.7 is sharp for $m \leqslant 2$ and $q=7,11$, $m=3,4$.

6. Conclusion and outlook

For the study of discrete structures the knowledge of their automorphism group is very important. In Section 3 we have completed the determination of the automorphism group of $\mathbb{F}_q^m$ with respect to integral distances.

The graphs $\mathfrak{G}_{q,m}$ of integral distances are interesting combinatorial objects. We were able to determine a few parameters and properties, but the large part remains unsettled. It would be nice to have a proof of Conjecture 4.6, which maybe is not too difficult. We would like to remark that for all dimensions $m \geqslant 3$ the graph of integral distances $\mathfrak{G}_{m,q}$ is at least a slight generalization of a strongly regular graph, a so-called three class association scheme.

Section 5 provides a first glimpse on the maximum cardinalities $\mathcal{I}(m,q)$ of integral point sets over $\mathbb{F}_q^m$. It remains a task for the future to determine some more exact numbers or lower and upper bounds. For small q we have no idea for a general construction of integral point sets with maximum

cardinality. A detailed analysis of the parameters of the 3-class association schemes including the eigenvalues of the corresponding graphs could be very useful to use some general upper bounds on clique sizes. A geometrical description of the point sets achieving $\mathcal{I}(3,q) = q+1$ for $q \equiv 3 \pmod 4$ would be interesting.

There are some similarities between integral point sets over $\mathbb{F}_q^m$ and integral point sets over Euclidean spaces $\mathbb{E}^m$. For example the constructions which lead to the maximum cardinality $\mathcal{I}(m,q)$ in $\mathbb{F}_q^m$ often coincide with the constructions which lead to integral point sets over $\mathbb{E}^m$ with minimum diameter, see [16,18,19].

Acknowledgment

We would like to thank the anonymous referee for many helpful comments to improve the presentation of the paper.

References

[1] A. Antonov, M. Brancheva, Algorithm for finding maximal Diophantine figures, Spring Conference 2007 of the Union of Bulgarian Mathematicians, 2007.
[2] A. Blokhuis, On subsets of $GF(q^2)$ with square differences, Indag. Math. (N.S.) 46 (1984) 369–372.
[3] A. Blokhuis, On subsets of $gf(q^2)$ with square differences, Indag. Math. (N.S.) 46 (1984) 369–372.
[4] A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme, T. Szőnyi, On the number of slopes of the graph of a function defined on a finite field, J. Combin. Theory Ser. A 86 (1) (1999) 187–196.
[5] P. Brass, W. Moser, J. Pach, Research Problems in Discrete Geometry, Springer-Verlag, 2005.
[6] S. Dimiev, A setting for a Diophantine distance geometry, Tensor (N.S.) 66 (3) (2005) 275–283; MR MR2189847.
[7] R.E. Fullerton, Integral distances in Banach spaces, Bull. Amer. Math. Soc. (N.S.) 55 (1949) 901–905.
[8] R.K. Guy, Unsolved Problems in Number Theory, second ed., Unsolved Problems in Intuitive Mathematics, vol. 1, Springer-Verlag, New York, NY, 1994, 285 p.
[9] H. Harborth, Integral distances in point sets, in: P.L. Butzer, et al. (Eds.), Karl der Grosse und sein Nachwirken, 1200 Jahre Kultur und Wissenschaft in Europa, in: Mathematisches Wissen., vol. 2, Brepols, Turnhout, 1998, pp. 213–224.
[10] B. Huppert, Endliche Gruppen. i, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, vol. 134, Springer-Verlag, Berlin, 1967, 793 p.
[11] M. Kiermaier, S. Kurz, Maximal integral point sets in affine planes over finite fields, Discrete Math., in press.
[12] M. Kleber, Encounter at far point, Math. Intelligencer 30 (1) (2008) 50–53.
[13] A. Kohnert, S. Kurz, Integral point sets over $\mathbb{Z}_n^m$, Electron. Notes Discrete Math. 27 (2006) 65–66.
[14] A. Kohnert and S. Kurz, Integral point sets over $\mathbb{Z}_n^m$, Discrete Appl. Math., in press.
[15] T. Kreisel, S. Kurz, There are integral heptagons, no three points on a line, no four on a circle, Discrete Comput. Geom. 39 (2008) 786–790.
[16] S. Kurz, Konstruktion und Eigenschaften ganzzahliger Punktmengen, PhD thesis, Bayreuth. Math. Schr., 76, Universität Bayreuth, 2006.
[17] S. Kurz, Integral point sets over finite fields, Australas. J. Combin. 43 (2009) 3–29.
[18] S. Kurz, R. Laue, Upper bounds for integral point sets, Australas. J. Combin. 39 (2007) 233–240.
[19] S. Kurz, A. Wassermann, On the minimum diameter of plane integral point sets, Ars Combin., in press.
[20] S. Niskanen, P.R.J. Östergård, Cliquer user's guide, version 1.0, Tech. Report T48, Communications Laboratory, Helsinki University of Technology, Espoo, Finland, 2003.
[21] L. Rédei, Lückenhafte polynome über endlichen Körpern (Gap Polynomials over Finite Fields), Math. Reihe, vol. 42, Birkhäuser-Verlag, Basel, 1970, 270 S.
[22] P. Sziklai, Directions in AG$(3,p)$ and their applications, Note Mat. 26 (1) (2006) 121–130.
[23] D.E. Taylor, The Geometry of the Classical Groups, Sigma Ser. Pure Math., vol. 9, Heldermann-Verlag, Berlin, 1992.
[24] D.B. West, Introduction to Graph Theory, second ed., Prentice Hall of India, New Delhi, 2005, 608 p.